TRANSMITTAL OF APPEAL BRIEF

Docket No. C0011/7002

Applicant:	Christopher J. Howard, Peter S. Levy and Joshue D. de la Cuesta
Serial No:	09/393,405
Filed:	September 10, 1999
For:	LIMITED-USE BROWSER AND SECURITY SYSTEM
Examiner:	P. Elisca
Art Unit:	3621

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being placed in the United States mail with first-class postage attached, addressed to Mail Stop Appeal Brief - Patents, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 on August 11, 2004.

Beverly Strasnick

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Transmitted herewith, in triplicate, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on 24 June 2004.

Status of Applicant

This application is on behalf of Copyright Clearance Center, Inc.

☒ Applicant claims small entity status.

Fee Due

Appeal Brief Fee	330.00
50% reduction for small entity	165.00
TOTAL FEE	165.00

Payment

☒ Enclosed is a check in the amount of the total fee.

☐ The Commissioner is authorized to charge the total fee to Deposit Account No. 02-3038.

☒ The Commissioner is hereby authorized to charge any other fees under 37 C.F.R. §1.16 and §1.17 that may be required, or credit any overpayment, to Deposit Account No. 02-3038. A duplicate of this transmittal letter is attached.

Paul D. Sorkin

Date: August 11, 2004

Paul D. Sorkin, Esq. Reg. No. 39,039
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656

IFW AF

APPELLANT'S BRIEF UNDER 37 CFR §1.192	Docket No. C0011/7002

Applicant:	Christopher J. Howard, Peter S. Levy and Joshue D. de la Cuesta
Serial No:	09/393,405
Filed:	September 10, 1999
For:	LIMITED-USE BROWSER AND SECURITY SYSTEM
Examiner:	Elisca, Pierre E.
Art Unit:	3621

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being placed in the United States mail with first-class postage attached, addressed to Mail Stop Appeal Brief - Patents, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 on August 11, 2004.

Beverly Strasnick

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

This brief is in furtherance of the Notice of Appeal, filed in this case on 24 June 2004.

The fees required under § 1.17(c), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief is transmitted in triplicate (37 C.F.R. 1.192(a)) and contains these items under the following headings, and in the order set forth below (37 C.F.R. 1.192(c)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF INVENTION
VI ISSUES
VII GROUPING OF CLAIMS
VIII ARGUMENTS
IX APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

I. REAL PARTY IN INTEREST (37 C.F.R. 1.192(c)(1))

The real party in interest in this appeal is Copyright Clearance Center, Inc., Danvers, Massachusetts.

II. RELATED APPEALS AND INTERFERENCES (37 C.F.R. 1.192(c)(2))

There are no other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on, the Board's decision in the pending appeal.

III. STATUS OF CLAIMS (37 C.F.R. 1.192(c)(3))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-112

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims pending: 24-43, 62-64, 78 and 95-112
2. Claims canceled: 1-23, 44-61, 65-77 and 79-94
3. Claims withdrawn from consideration, but not canceled: none
4. Claims allowed: none
5. Claims rejected: 24-43, 62-64, 78 and 95-112

C. CLAIMS ON APPEAL

The claims on appeal are 24-43, 62-64, 78 and 95-112

IV. STATUS OF AMENDMENTS (37 C.F.R. 1.192(c)(4))

In the amendment filed 15 December 2003, Appellant canceled claims 79 and 80 and added claims 111 and 112. It appears that the Examiner missed these claims amendments. As a result, Appellant respectfully submits that claims 24-43, 62-64, 78 and 95-112 are pending in the application contrary to the listing of claims in the Office Action dated 24 March 2004.

V. SUMMARY OF INVENTION (37 C.F.R. 1.192(c)(5))

The present invention is directed to a security system that allows a content provider to publish content on a local-area network (LAN) or wide-area network (WAN), such as the World Wide Web (web) and the Internet, while safeguarding its intellectual property against misuse by unauthorized organizations or individuals. The present invention allows the content provider to control use of the content by disabling functions of a web browser that would otherwise facilitate the sharing of the content. The invention can be implemented as a stand-alone web browser, or as an add-in security module, such as a plug-in or control, to be embedded into an existing web browser, including general purpose browsers such as Microsoft's Internet Explorer and Netscape's Navigator, or proprietary browsers such as that provided by America Online for its subscribers. (P. 6, lines 18 – 26.)

This system permits a source to download content for previewing by a user without fully releasing the content for general use because the source controls which functions can be performed by the browser. Advantageously, the system does not require special passwords or other methods of user authentication. The security system secures the content at the source and only permits it to be downloaded to a client computer running a limited-user browser or a general-purpose browser executing an add-in security module providing the same functions as a limited-user browser.

The limited-use web browser/add-in security module of the present invention reads and displays any viewable web content including text, images and streaming audio and video but limits the user to an ephemeral view or presentation of the information. Ephemeral output is visual or audio output that cannot be electronically reproduced or otherwise communicated by a computer system. (P. 7, lines 10-17.) The browser secures the downloaded content on the client computer and displays it in a "view-only" mode.

The mechanism by which the browser is disabled varies in accordance with different embodiments of the invention. In one embodiment, the plug-in module that converts a standard browser to a limited use browser is downloaded from a source or publisher. (P. 16, lines 24-27.) In another embodiment, information that controls how

content is viewed arrives at the user's browser in a secure document that also contains the content. (P. 19, lines 21-26 and P. 21, lines 16-26.)

The restrictions on the browser also depend on the particular embodiment. In one embodiment, all forms of non-ephemeral reproduction, e.g., printing, saving to disk, etc., are disabled. While the secured content is being displayed, menu selections, key combinations, or pointing device commands initiated on the client computer that would modify the content or create a copy on another medium are either disabled by default or monitored to determine if the action is permitted. The protected content can be displayed in a window within the browser frame or in a separate window having a special control set.

One embodiment of the present invention is described in conjunction with an example illustrated in FIG. 3 in which the invention is divided into three components. The first component is the limited-use web browser (or add-in security module) executing on a client. The second component is a server security module executing on a server that handles the distribution of web content over a LAN or a WAN. The third component comprises two security models for protecting the content: an "individual" security model that uses a secure document package and a "common" security model that uses encryption. The security models have both client and server elements. (P.12, lines 17-27).

In one embodiment, the secure document package is a dynamically compiled executable that combines web content data with the ability to control and manipulate it. The server security component builds the secure document package and the limited-use browser/add-in security module runs it. In another embodiment, the server security component creates and transmits a stream of encrypted content to the client computer and the limited-use browser/add-in security module decrypts the content and displays it.

The server and client digital processing systems of the present invention implement different techniques to prevent the unauthorized copying of web content.

These different techniques include:

1) Window Subclassing - the client digital processing system intercepts and processes messages sent or posted before the destination window has an opportunity to process them. By subclassing a window, the client can monitor the behavior of the

window, including key strokes input into the window. If the limited-use browser or add-in security module is not the foreground application, a message for an unauthorized function is discarded or the content is hidden from view.

2) Clipboard Flushing - stops a user from sending a screen-capture to the clipboard by continuously destroying the contents of the clipboard while the web browser is the active application. This technique also prevents background applications from copying the screen contents to the clipboard.

3) Disabling of Browser functions - the limited-use browser on the client computer typically is implemented with no menu items, keystrokes, or mouse actions that can copy, save, or print or otherwise produce a non-ephemeral reproduction. There can optionally be selective control or activation of these functions embedded in a secure document package. If a web content owner authorizes a web page to be printed but not saved, the print function can be made available to the user, or if a particular user is allowed by a particular content owner to produce non-ephemeral reproductions, the corresponding functions can be activated.

4) Source Code Encryption - the HTML source code is encrypted by the server digital processing system using a system level encryption (SLE) key and the client digital processing system does not allow viewing or saving unencrypted HTML source code.

5) User Level Encryption - a unique identifier, ULE key, is created when the limited-use browser or add-in security module is installed on the client computer. Downloaded content is localized to the client digital processing system by encrypting the content with the ULE key. The ULE key is created either directly or algorithmically from a machine ID for the client computer.

6) Secure Document Package - a secure document package is composed of a document manager and one or more web pages, each of which is encrypted with the ULE. To decrypt the package, it is necessary to know where to break up the individual pages before attempting to decrypt the file and even then encryption makes the content unusable to anyone but the owner of the machine with the client registered with the unique ULE key.

7) Disabling "Drag & Drop" - the ability to "drag & drop" an image or object within a web page is not available in the limited-use browser or a browser equipped with the add-in security module.

8) Secure Cache Content - all web content downloaded and stored on the client computer in the course of browsing the web, known as cached content, is secured from the user through encryption.

9) Device Context Monitoring - checks the context for each input/output device against the secured image or text to determine if protected content is being accessed by the device. (P. 18, line 18 – P. 20, line 9.)

VI. ISSUES (37 C.F.R. 1.192(c)(6))

I. Whether claims 24-43, 62-64, 78 and 95-112 are patentable over Dykes et al., U.S. Pat. No. 5,872,915, (hereinafter "Dykes") in view of Maddalozzo et al., U.S. Pat. No. 6,460,060, (hereinafter "Maddalozzo") under 35 U.S.C. § 103(a).

VII. GROUPING OF CLAIMS (37 C.F.R. 1.192(c)(7))

Group I, claims 24, 30-39, 41-43, 111 and 112 stand together.
Group II, claim 25 stands alone.
Group III, claim 26 stands alone.
Group IV, claim 27 stands alone.
Group V, claim 28 stands alone.
Group VI, claim 29 stands alone.
Group VII, claims 40, 62-64 and 78 stand together.
Group VIII, claims 95-103 stand together.
Group IX, claims 104-110 stand together.

VIII. ARGUMENT (37 C.F.R. 1.192(c)(8))

A. Prima facie obviousness has not been established because there has been no showing of motivation to combine Dykes and Maddalozzo.

Obviousness is a legal conclusion based on factual evidence. Graham v. John Deere Co. 383 US 1, 148 USPQ 459 (1966). The PTO has the burden under 35 U.S.C. §103 to establish a prima facie case of obviousness. In re Piasecki, 745 F.2d 1468, 1471-72, 223 USPQ 785, 787-87 (Fed. Cir. 1984). In order to establish the prima facie case of obviousness, the teaching or suggestion to make the claimed combination and

the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991.) There are three possible sources for a motivation to combine references: the nature of the problem to be solved, the teachings of the prior art and the knowledge of persons of ordinary skill in the art. In re Rouffet, 149 F.3d 1350, 1357, 47 USPQ2d 1453, 1457-1458 (Fed. Cir. 1998.)

Dykes is directed to an authentication system that reduces the number of times a user has to send authentication information to a network server to access application programs running on the server. The user inputs data into a standard web browser, such as Netscape or Microsoft Internet Explorer, that causes the user's computer to send a request for access to a remote application program to a web server application. The web server application receives the access request and, in response, requests the user input identifying information, e.g., a user ID, password and a key, which the web server application uses to authenticate the user. The key specifies the particular remote application program the user wishes to access. The web server application uses the user ID and password to authenticate the user and passes the user ID and key to an application gateway if the user is authenticated. The application gateway searches a user library for a matching user ID and key. If the application gateway finds a match, it logs onto the application program using the information in the user library and translates the user input into commands for the application program. The application program responds by sending data to the application gateway which translates data into output that can be handled by the browser and then, in turn, passes the data back to the browser for display to the user.

Maddalozzo is not related to limiting access to a computer system or application to only authorized users but, rather, is directed to automatically generating a search list from URLs as found in the history and bookmark information of a web browser. More specifically, Maddalozzo relates to a method and system for automatically providing a pertinent list of previously visited web pages that can be searched based on specific parameters defined by a user. Maddalozzo further describes a method for automatically searching previously visited web pages, that are not bookmarked, for specified key words or for searching multiple pages visited during a specified period, whether stored

in the cache on a data processing system or accessibly only on the Internet. Maddalozzo describes automatically generating a search list of web sites to be searched, from URLs in the browser's bookmark and/or history files and then automatically accessing and searching each URL on the Internet or cache on the browser's computer. As a result, Maddalozzo automatically searches those sites that a user may have previously visited, but not recorded as a bookmark, in order to provide a higher likelihood that the information for which the user is searching can be found in recently visited web site locations.

It is clear that there is no motivation for the Examiner's proposed combination of Dykes and Maddalozzo. Dykes is directed to providing secure access to a software application from a web browser, whereas Maddalozzo is directed to keeping track of web sites that have been visited by a user in order to more efficiently search and find desired information. These problems clearly are not the same. The Dykes system does not need to keep track of previously visited web sites in order to find information because Dykes is concerned with limiting access to an application program only to authorized users. Maddalozzo is totally unrelated to the problems of insuring that only authorized users gain access to application programs. Consequently, there would be no motivation for one skilled in art to combine these references that flows from the nature of the problem to be solved because each of these references is directed to a different problem.

Further, neither reference suggests such a combination. Dykes is not directed to keeping track of miscellaneous web site that have been visited, but not bookmarked, and the issues involved in identifying where desired information may be located. Maddalozzo, as submitted above, is not concerned with authorizing access to software applications.

The Examiner suggests that

> ...it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the software applications of Dykes by including the limitation detailed above as taught by Maddalozzo because this would restrict unauthorized downloading content access. (Final office action, 24 March 2004, page 2)

The Examiner has the burden, however, to make particular findings as to the reason why a skilled artisan, with no knowledge of the claimed invention, would have selected the suggested components for combination in the manner claimed. In re Rouffett, *Supra* at 1359, 1459. In the final office action, the Examiner has stated only a general "improvement" that, by itself, cannot suggest selecting the particular references cited and combining them in a manner to produce the claimed invention.

Accordingly, Appellant respectfully submits that the cited combination of Dykes and Maddalozzo is improper and should be withdrawn.

B. Prima facie obviousness has not been established because the combination of Dykes and Maddalozzo does not teach or suggest the structure recited in the Group I claims.

To establish the prima facie obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1970). Assuming, without agreeing, that the combination of Dykes and Maddalozzo is proper, the combination still does not teach or suggest the limitations recited in the Group I claims.

The Examiner has cited the same sections of Dykes as specified in prior office actions as the basis for withdrawn rejections under 35 USC §102(e). In setting forth the current rejection under §103, the Examiner has stated:

> Dykes substantially discloses a computer system/method for providing security checking for software applications access via the www (which is readable as applicant's claimed invention wherein it is stated that a method for controlling access to information presented by a web browser executing on a local computer system connected to a computer network), comprising: presenting content within a browser window of the web browser **(See, Abstract lines 1-10, column 3, lines 22-58, column 4, lines 47-57, please note that NETSCAPE is capable of presenting content or object within a browser window of the web browser); and** disabling at the local computer system or on the client digital processing system a disallowed user function when the content is within the browser window **(See, Abstract, lines 1-10, column 3, lines 22-58, column 4, lines 47-57, please note that NETSCAPE is capable of disabling and disallowed user function).** (emphasis in original)

The present invention concerns a security system that allows the user to download content from a source to a web browser. The security system secures the content at the source and only permits it to be downloaded to a client computer running a limited-use browser or a general-purpose browser executing an add-in security module providing the same functions as the limited-use browser. The browser secures the downloaded content in the client computer and displays it in a "view-only" mode. This system permits a source to download content for previewing by a user without fully releasing the content for general use because the source controls what functions can be performed by the browser. Advantageously, the system requires no special passwords or other user authentication.

Claim 24 is representative of the claims in Group I and recites a method for controlling access to information presented by a web browser executing on a local computer system connected to a computer network wherein the content is downloaded from a source over the computer network to the web browser. Further, as recited in claim 1, authorization information is downloaded from the source to the web browser that configures the web browser to process content in a manner determined by the source, content is downloaded from the source to the web browser and the downloaded content is presented within a browser window of the web browser. Finally, as determined by the source in accordance with the authorization information, disallowed user functions are disabled at the local computer system that affect the downloaded content when the downloaded content is within the browser window.

Dykes neither teaches nor discloses that local functions on the web browser are disabled in any manner. Dykes discloses a system for providing secure access to a software application. Once, however, a user in the Dykes system is granted access to the software application there is no restriction on the local computer system as to what can be done with the downloaded information. Specifically, there are no limitations on copying, forwarding or printing the downloaded information from the browser.

The Examiner asserts that "NETSCAPE is capable of disabling and [sic] disallowed user function." Despite written requests from Appellant to do so, the Examiner has failed to provide any evidence to support his contention that Netscape (presumably referring to the browser), as of February 8, 1999, was indeed capable of

disabling a user function. If the Examiner has support for this contention, Appellant requests that it be provided and formally presented in a new non-final office action on the merits. Without such support as to the capacity of Netscape, the Examiner's contention is unsupported and, Appellant respectfully submits, carries no weight as the basis for a rejection.

The Examiner acknowledges that Dykes fails to "explicitly disclose" the limitation wherein content is downloaded from a source over the computer network to the web browser. The Examiner cites Maddalozzo saying:

> Maddalozzo discloses a web browser having search capabilities automatically generates a search list of web cites wherein clients computer downloading web page and searching the content of said downloaded web page (downloaded web page or bookmark) utilizing said at least one user-input search parameter or software ... therefore it would have been obvious to a person of ordinary skill at the time the invention was made to modify the software application of Dykes by including the limitation detailed above as taught by Maddalozzo because this would restrict unauthorized downloading content access.

Maddalozzo does not remedy the deficiencies of Dykes. Appellant submits that a combination of Dykes and Maddalozzo will result in a system that control access to a software application by limiting access to only authorized users, as taught by Dykes, and would include a feature of keeping track of locations visited by a user on the web browser.

In contrast, claim 24 as representative of the Group I claims, as above, recites disabling at the local computer system a disallowed user function that affects the downloaded content when the downloaded content is within the browser window.

The cited combination of Dykes and Maddalozzo, however, does not teach or suggest disabling a disallowed user function. Thus, for at least this reason, the Group I claims are not rendered obvious by the cited combination.

C. Prima facie obviousness has not been established because the combination of Dykes and Maddalozzo does not teach or suggest the structure recited in the Group II claims.

Independent claim 25, the only claim in Group II, is directed to a method for controlling access to information presented by a web browser where the content is downloaded from a source over a computer network to the browser. Similar to claim 24, authorization information is downloaded along with the content from the source to the web browser, the downloaded content is presented and disallowed user functions, as determined by the source in accordance with the authorization information, are disabled. Independent claim 25, as different from claim 24, recites that the downloaded content is hidden if the browser is not a foreground application.

The cited combination of Dykes in view of Maddalozzo, however, does not teach or suggest a security system including the feature that the downloaded content is hidden if the browser is not a foreground application as is recited in claim 25. The Examiner has pointed to no portion of either reference that discloses the claimed method for controlling access.

Accordingly, Appellant respectfully submits that independent claim 25 is allowable over the cited combination of references.

D. Prima facie obviousness has not been established because the combination of Dykes and Maddalozzo does not teach or suggest the structure recited in the Group III claims.

Independent claim 26, the only claim in Group III, is directed to a method for controlling access to information, similar to that recited in claims 24 and 25. Independent claim 26, however, recites a step of disabling at the local computer system a disallowed user function when the downloaded content is within the browser window by clearing a commonly shared inter-application memory that can contain the downloaded content.

Similar to the argument submitted above with respect to the deficiencies of the cited combination, Appellant respectfully submits that there is no teaching or suggestion of a system that includes clearing a commonly shared inter-application memory in

accordance with authorization information that has been downloaded, all as recited in independent claim 26. Accordingly, Appellant respectfully submits that independent claim 26 is allowable over the cited combination of references.

E. Prima facie obviousness has not been established because the combination of Dykes and Maddalozzo does not teach or suggest the structure recited in the Group IV claims.

Independent claim 27 is the only claim in Group IV and is directed to a method of controlling access, including the steps of downloading web browser authorization information from a source to a web browser that configures the web browser, downloading content from the source to the web browser and presenting the downloaded content within the browser window of the web browser. Claim 27 further recites the disallowed user function is disabled, as determined by the source in accordance with the authorization information, when the downloaded content is within the browser window by hiding a user menu selection that affects the downloaded content corresponding to the disallowed user function.

Appellant respectfully submits that the cited combination does not teach or suggest the method for controlling access to information, as recited in independent claim 27, including disabling the disallowed user function by hiding a user menu selection. The Examiner has failed to identify where the cited combination discloses all of the limitations of the invention as recited in claim 27.

Accordingly, Appellant submits that independent claim 27 is allowable over the cited combination of references.

F. Prima facie obviousness has not been established because the combination of Dykes and Maddalozzo does not teach or suggest the structure recited in the Group V claims.

Independent claim 28, the only claim in Group V, is directed to a method for controlling access to information presented by a web browser where content is downloaded from a source over a computer network to the web browser. The method comprises, similar to that as recited in claims 24-27, downloading from the source to the

web browser authorization information that configures the web browser to process content in a manner determined by the source, downloading content from the source to the web browser and presenting the downloaded content within a browser window of the web browser. Further, as determined by the source in accordance with the authorization information, a disallowed user function is disabled at the local computer system when the downloaded content is within the browser window by intercepting a keyboard message that affects the downloaded content and discarding the keyboard message if it corresponds to the disallowed user function.

The cited combination of Dykes in view of Maddalozzo fails to teach or suggest the method for controlling access to information as recited in claim 28, because the combination fails to teach or suggest each and every limitation recited in the claim. At a minimum, the cited combination fails to teach or suggest intercepting a keyboard message that affects the downloaded content in order to disable a disallowed user function in accordance with authorization information and, further, discarding the keyboard message if it corresponds to the disallowed user function. Appellant respectfully submits that the cited combination utterly fails to render obvious that which is recited in claim 28 and submits that independent claim 28 is allowable over the cited combination of references.

G. Prima facie obviousness has not been established because the combination of Dykes and Maddalozzo does not teach or suggest the structure recited in the Group VI claims.

Independent claim 29, the only claim in Group VI, is directed to a method for controlling access to information presented by a web browser, and, similar to the preceding claims 24-28, comprises downloading from a source to a web browser authorization information that configures the web browser to process content in a manner determined by the source, downloading content from the source to the web browser and presenting the downloaded content within a browser window. Further, as determined by the source in accordance with the authorization information, the method comprises disabling at the local computer system a disallowed user function when the downloaded content is within the browser window by monitoring a context for a device

and discarding a user's action directed to the device when the context matches the downloaded content.

Appellant submits that claim 29 is allowable over the cited combination for at least the reason that the cited combination fails to teach or suggest disabling a disallowed user function at a local computer system when the downloaded content is within the browser window by monitoring a context for a device and discarding the user action directed to the device when the context matches the downloaded content. Appellant respectfully submits that the obviousness rejection based on the combination cannot be maintained.

H. Prima facie obviousness has not been established because the combination of Dykes and Maddalozzo does not teach or suggest the structure as recited in the Group VII claims.

Independent claim 40 is representative of the Group VII claims. Claim 40 is directed to a method for controlling access to information presented by a web browser where content is downloaded from a source over a computer network to the web browser. The method comprises downloading authorization information that configures the web browser to process content in a manner determined by the source and downloading content from the source to the web browser. Further, the downloaded content is presented within a browser window of the web browser and, as determined by the source in accordance with the authorization information, disabling at the local computer system when the downloaded content is within the window browser, a user function that provides for non-ephemeral reproduction of the content.

To reiterate, Dykes discloses a system for controlling access to a software application in order to ensure that only authorized users gain access. Maddalozzo discloses a system for tracking and/or retrieving information regarding web sites that a user has visited in order to make searching more efficient. The cited combination, however, fails to teach or suggest a method as recited in claim 40, including at least disabling a user function that provides for non-ephemeral reproduction of the content at the local computer system when the downloaded content is within the browser window.

Appellant respectfully submits that, for at least the reason that the cited combination does not teach or disclose each and every limitation of representative claim 40, all of the Group VII claims are allowable.

I. Prima facie obviousness has not been established because the combination of Dykes and Maddalozzo does not teach or suggest the structure as recited in the Group VIII claims.

Independent claim 95 is representative of the Group VIII claims. Claim 95 is directed to a method in a local computer system operatively connectable to a source of content and capable of executing a web browser and a viewer program that runs within the web browser. The viewer program has a plurality of functions related to presenting the content from the source where the method comprises downloading the viewer program from the source, receiving from the source function authorization data indicating which of the viewer functions may be performed at the local computer system on the content and receiving content from the source. Further, the method includes presenting the content with the viewer program and disabling, at the local computer system, selected viewer functions in accordance with the function authorization data received from the source.

The cited combination of Dykes in view of Maddalozzo fails to teach or suggest the method as recited in claim 95 because the combination fails to teach or suggest each and every limitation recited in the claim. At a minimum, the cited combination fails to teach or suggest a viewer program that runs within a web browser where the viewer program has a plurality of functions for presenting the content and, further, where selected viewer functions are disabled in accordance with the authorization data.

Appellant respectfully submits that, for at least the reason that the cited combination does not teach or disclose each and every limitation of representative claim 95, all of the Group VIII claims are allowable.

J. Prima facie obviousness has not been established because the combination of Dykes and Maddalozzo does not teach or suggest the structure as recited in the Group IX claims.

Independent claim 104 is representative of the Group IX claims. Claim 104 is directed to a method in a local computer system operatively connected to a source of content and capable of executing a presentation program where the presentation program has a plurality of functions related to presenting the content from the source. The method comprises receiving a document containing function authorization data and content from the source where the function authorization data specifies which presentation program functions are enabled and disabled and displaying the content with the presentation program. Further, the method includes monitoring user command input to the presentation program and selectively enabling at the local computer system presentation program functions in accordance with the function authorization data received from the source.

To recap, Dykes describes a system for controlling application access in order to ensure that only authorized users gain access. Maddalozzo discloses a system for tracking web sites that a user has visited in order to make searching more efficient. The cited combination, however, fails to teach or suggest a method as recited in claim 104, including at least running a presentation program, receiving a document containing function authorization, monitoring user input to the presentation program and selectively enabling presentation program functions in accordance with the authorization data.

Appellant respectfully submits that, for at least the foregoing reason, claim 104 and the other Group IX claims are allowable.

K. CONCLUSION

Appellant's claimed invention is unobvious over the cited art where the art fails to disclose many of the claimed features. The cited prior art does not suggest any combination or modification that would yield the invention disclosed and claimed. The cited prior art in and of itself and without the benefit of Appellant's disclosure does not support the conclusion that the invention defined by the appealed claims is obvious.

Respectfully submitted,

Date: August 11, 2004

Paul D. Sorkin, Esq. Reg. No. 39,039
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656

IX APPENDIX OF CLAIMS (37 C.F.R. 1.192(c)(9))

The text of the claims involved in the appeal is:

24. A method for controlling access to information presented by a web browser executing on a local computer system connected to a computer network, wherein content is downloaded from a source over the computer network to the web browser, the method comprising:

downloading from the source to the web browser authorization information that configures the web browser to process content in a manner determined by the source;

downloading content from the source to the web browser;

presenting the downloaded content within a browser window of the web browser; and

as determined by the source in accordance with the authorization information, disabling at the local computer system a disallowed user function that affects the downloaded content when the downloaded content is within the browser window.

25. A method for controlling access to information presented by a web browser executing on a local computer system connected to a computer network, wherein content is downloaded from a source over the computer network to the web browser, the method comprising:

downloading from the source to the web browser authorization information that configures the web browser to process content in a manner determined by the source;

downloading content from the source to the web browser;

presenting the downloaded content within a browser window of the web browser;

as determined by the source in accordance with the authorization information, disabling at the local computer system a disallowed user function

when the downloaded content is within the browser window by intercepting a message posted to the browser window; and

hiding the downloaded content if the browser is not a foreground application.

26. A method for controlling access to information presented by a web browser executing on a local computer system connected to a computer network, wherein content is downloaded from a source over the computer network to the web browser, the method comprising:

downloading from the source to the web browser authorization information that configures the web browser to process content in a manner determined by the source;

downloading content from the source to the web browser;

presenting the downloaded content within a browser window of the web browser; and

as determined by the source in accordance with the authorization information, disabling at the local computer system a disallowed user function when the downloaded content is within the browser window by clearing a commonly shared inter-application memory that can contain the downloaded content.

27. A method for controlling access to information presented by a web browser executing on a local computer system connected to a computer network, wherein content is downloaded from a source over the computer network to the web browser, the method comprising:

downloading from the source to the web browser authorization information that configures the web browser

downloading content from the source to the web browser;

presenting the downloaded content within a browser window of the web browser; and

as determined by the source in accordance with the authorization information, disabling at the local computer system a disallowed user function when the downloaded content is within the browser window by hiding a user menu selection that affects the downloaded content corresponding to the disallowed user function.

28. A method for controlling access to information presented by a web browser executing on a local computer system connected to a computer network, wherein content is downloaded from a source over the computer network to the web browser, the method comprising:

downloading from the source to the web browser authorization information that configures the web browser to process content in a manner determined by the source;

downloading content from the source to the web browser;

presenting the downloaded content within a browser window of the web browser;

as determined by the source in accordance with the authorization information, disabling at the local computer system a disallowed user function when the downloaded content is within the browser window by intercepting a keyboard message that affects the downloaded content; and

discarding the keyboard message if it corresponds to the disallowed user function.

29. A method for controlling access to information presented by a web browser executing on a local computer system connected to a computer network, wherein content is downloaded from a source over the computer network to the web browser, the method comprising:

downloading from the source to the web browser authorization information that configures the web browser to process content in a manner determined by the source;

downloading content from the source to the web browser;

presenting the downloaded content within a browser window of the web browser;

as determined by the source in accordance with the authorization information, disabling at the local computer system a disallowed user function when the downloaded content is within the browser window by monitoring a context for a device; and

discarding a user action directed to the device when the context matches the downloaded content.

30. The method of claim 24, wherein the disallowed user function is one of a plurality of default disallowed user functions and further comprising:
leaving active one of the plurality of default disallowed user functions.

31. The method of 30, further comprising providing information with the downloaded content that determines the one of the plurality of default disallowed user functions to be left active.

32. The method of claim 24 wherein the disallowed user function is selected from the group consisting of print, page setup, save, save as, view source, save picture as, set as wallpaper, copy, screen capture, screen print, cut.

33. The method of claim 24 further comprising managing authentication of a web client.

34. The method of claim 24 further comprising processing a request from a web client for encrypted content.

35. The method of claim 24 further comprising creating a unique identifier for a web client.

36. The method of claim 24 further comprising encrypting content before downloading with a key based on the unique identifier for the web client.

37. The method of claim 24 wherein the downloaded content comprises user perceivable information in a hyper-text markup language (HTML) format.

38. The method of claim24 wherein the downloaded content comprises user perceivable streaming information.

39. The method of claim 24 wherein the downloaded content comprises at least one of video information and audio information.

40. A method for controlling access to information presented by a web browser executing on a local computer system connected to a computer network, wherein content is downloaded from a source over the computer network to the web browser, the method comprising:

downloading from the source to the web browser authorization information that configures the web browser to process content in a manner determined by the source;

downloading content from the source to the web browser;

presenting the downloaded content within a browser window of the web browser; and

as determined by the source in accordance with the authorization information, disabling at the local computer system when the downloaded content is within the browser window, a user function that provides for non-ephemeral reproduction of the content.

41. The method of claim 24 wherein the downloaded content comprises user perceivable information in a scripting language format.

42. The method of claim 24 wherein the downloaded content comprises user perceivable information in a common gateway interface (CGI) language format.

43. The method of claim 24 wherein the downloaded content comprises user perceivable information in a JAVA language format.

62. A computer readable medium having stored thereon computer executable instructions to cause a client digital processing system to perform a method comprising:

receiving from a server digital processing system in a browser window client executing on the client digital processing system authorization information that configures the browser window client to process content in a manner determined by the server digital processing system;

receiving protected content from the server digital processing system;

presenting the protected content within the browser window client executing on the client digital processing system; and

as determined by the server digital processing system in accordance with the authorization information, disabling at the client digital processing system disallowed user functions when the protected content is in the browser window, wherein the disallowed user function comprises a user function which, when allowed, provides for non-ephemeral reproduction of the protected content.

63. The computer-readable medium of claim 62 wherein the medium has stored thereon computer executable instructions to cause the client digital processing system to perform the method further comprising:

intercepting a message posted to the browser window; and hiding the protected content if the browser is not a foreground application.

64. A computer readable medium of claim 62 wherein the medium has stored thereon computer executable instructions to cause the client digital processing system to perform the method in which the disallowed user function is enabled when

content in the browser window is not designated to be protected such that non-ephemeral reproduction of such content is allowed.

78. A system for controlling reproduction of content downloaded from a source over a network to a client computer system comprising:

means for receiving from the source, authorization information that configures a web browser executing in the client computer system to process content in a manner determined by the source;

means responsive to the authorization information for modifying the web browser to prevent the web browser from being used to reproduce, in at least one form, content received by the web browser;

means for receiving at the client computer system the downloaded content to be protected; and

means for displaying in the web browser the protected content .

95. In a local computer system operatively connectable to a source of content and capable of executing a web browser and a viewer program that runs within the web browser, the viewer program having a plurality of functions related to presenting the content from the source, a method comprising:

(A) downloading the viewer program from the source;

(B) receiving from the source function authorization data indicating which of the viewer functions may be performed at the local computer system on the content;

(C) receiving content from the source;

(D) presenting the content with the viewer program; and

(E) disabling at the local computer system selected viewer functions in accordance with the function authorization data received from the source.

96. The method of claim 95 wherein the disabled viewer functions are selected from the group consisting of print, page set-up, save, save as, view source, save picture as, set as wallpaper, copy, screen capture, print screen and cut functions.

97. The method of claim 95 wherein the viewer program comprises an add-in security module that modifies the web browser at the local computer system.

98. A computer program product for use with a local computer system operatively coupled to a source of content, the local computer system capable of executing a web browser and a viewer program that runs within the web browser, the viewer program having a plurality of functions related to presenting the content from the source, the computer program product comprising a computer useable medium having embodied therein program code comprising:

(A) program code for downloading the viewer program from the source;

(B) program code for receiving from the source function authorization data indicating which of the viewer functions may be performed at the local computer system on the content ;

(C) program code for receiving content from the source;

(D) program code for presenting the content with the viewer program; and

(E) program code for disabling at the local computer system selected viewer functions in accordance with the function authorization data received from the source.

99. The computer program product of claim 98 wherein the disabled viewer functions are selected from the group consisting of print, page set-up, save, save as, view source, save picture as, set as wallpaper, copy, screen capture, print screen and cut functions.

100. The computer program product of claim 98 wherein the viewer program comprises an add-in security module that modifies the web browser at the local computer system.

101. Apparatus for use with a local computer system operatively coupled to a source of content, the computer system capable of executing a web browser and a viewer

program that runs within the web browser, the viewer program having a plurality of functions related to presenting the content from the source, the apparatus comprising:

(A) a processor;

(B) a memory coupled to the processor;

(C) a network interface coupled to the processor and the memory;

(D) program logic for downloading the viewer program from the source;

(E) program logic for receiving from the source function authorization data indicating which of the viewer functions may be performed at the local computer system on the content ;

(F) program logic for receiving content from the source;

(G) program logic for presenting the content with the viewer program; and

(H) program logic for disabling at the local computer system selected viewer functions in accordance with the function authorization data received from the source.

102. The apparatus of claim 101 wherein the disabled viewer functions are selected from the group consisting of print, page set-up, save, save as, view source, save picture as, set as wallpaper, copy, screen capture, print screen and cut functions.

103. The apparatus of claim 101 wherein the viewer program comprises an add-in security module that modifies the web browser.

104. In a local computer system operatively connected to a source of content and capable of executing a presentation program, the presentation program having a plurality of functions related to presenting the content from the source, a method comprising:

(A) receiving a document containing function authorization data and content from the source, the function authorization data specifying which presentation program functions are enabled and disabled;

(B) displaying the content with the presentation program;

(C) monitoring user command input to the presentation program; and

(D) selectively enabling at the local computer system presentation program functions in accordance with the function authorization data received from the source.

105. The method of claim 104 wherein (D) comprises:

(D1) determining if the authorization data associated with the content defines restrictions on the presentation program functions;

(D2) if restrictions are defined, disallowing at the local computer system selected program functions; and

(D3) if no restrictions are defined, allowing at the local computer system all presentation program functions.

106. The method of claim 104 wherein the disallowed user functions are selected from the group consisting of print, page set-up, save, save as, view source, save picture as, set as wallpaper, copy, screen capture, print screen and cut functions.

107. In a local computer system operatively connected to a source of content and capable of executing a presentation program, the presentation program having a plurality of functions related to presenting the content from the source, a method comprising:

(A) receiving a document containing authorization information and content from the source, the authorization information specifying which presentation program functions are enabled and disabled;

(B) displaying the content with the presentation program;

(C) monitoring user command input to the presentation program; and

(D) using the authorization information to enable at the local computer system less than all of the presentation program functions while the content is being presented.

108. The method of claim 107 wherein the disallowed user functions are selected from the group consisting of print, page set-up, save, save as, view source, save picture as, set as wallpaper, copy, screen capture, print screen and cut functions.

109. In a local computer system operatively connected to a source of content and capable of executing a presentation program, the presentation program capable of presenting the content from the source, a method comprising:

(A) running the presentation program in a web browser executing on the local computer system;

(B) receiving a document containing authorization information and content from the source, the authorization information specifying which presentation program functions are enabled and disabled;

(C) displaying the content with the presentation program; and

(D) using the authorization information to control the presentation program to prevent non-ephemeral reproduction of the content being displayed with the presentation program.

110. The method of claim 109 wherein (D) comprises:

(D1) limiting at the local computer system user control over the content through a technique selected from the group consisting of window subclassing, clipboard flushing, disabling of browser functions, source code encryption, user level encryption, document package securing, drag and drop disabling, cache content securing, and device context monitoring.

111. The method of claim 24 wherein the authorization information comprises a plug-in program that is downloaded before the content is downloaded.

112. The method of claim 24 wherein the authorization information is part of a document that includes the content.